The Global Protection of Personal Health Data

Peter R Croll[a], Pekka Ruotsalainen[b], Eike-Henner W Kluge[c], Bernd Blobel[d], Najeeb Al-Shorbaji[e], Paulette Lacroix[f], Tony Sahama[g], Mauro Giacomini[h], Kiyomu Ishikawa[i]

[a] Health Informatics Society of Australia, VIC, Australia
[b] Tampere University, Finland
[c] University of Victoria, Victoria, BC, Canada
[d] Medical Faculty, University of Regensburg, Germany
[e] World Health Organization (WHO) Geneva, Switzerland
[f] PC Lacroix Consulting Inc, North Vancouver, BC, Canada
[g] Queensland University of Technology, QLD, Australia
[h] DIBRIS, University of Genova, Italy
[i] Hiroshima University, Japan

Abstract

The workshop is an activity of the IMIA Working Group 'Security in Health Information Systems' (SiHIS). It is focused to the growing global problem: how to protect personal health data in today's global eHealth and digital health environment. It will review available trust building mechanisms, security measures and privacy policies. Technology alone does not solve this complex problem and current protection policies and legislation are considered woefully inadequate. Among other trust building tools, certification and accreditation mechanisms are discussed in detail and the workshop will determine their acceptance and quality. The need for further research and international collective action are discussed. This workshop provides an opportunity to address a critical growing problem and make pragmatic proposals for sustainable and effective solutions for global eHealth and digital health.

Keywords:

Electronic medical record; personal health information systems, information security; privacy; trust; data sharing; certification, accreditation; medical tourism, digital health.

Workshop Description

It is widely recognised that privacy of our most sensitive health information is of paramount importance [1]. It is also the key enabler for global healthcare and digital health. Yet health information systems are not as secure as banks with evidence indicating that data breaches are increasing at an alarming rate [2]. Digital health applications are based on the use of unsecure Internet and global Cloud services. The secondary use of health data is increasing rapidly and the collection of Personal Health Information (PHI) is difficult or even impossible to control on an individual level. Many organisations offering healthcare and health services operate within countries that have little to no legislation to protect privacy. This is compounded by the fact that health information is highly sensitive requiring special protections and therefore healthcare cannot be treated like other industry sectors [3].

Medical tourism is a huge growth industry that is now attracting widespread support from health insurers looking to reduce their costs within acceptable health and safety standards. Typically, patients are travelling from more prosperous countries to lower cost third world countries that now offer high quality healthcare service. They can expect to pay as little as 20% of the price for medical services compared with their own country [4]. When touring, patients from Western nations will rarely experience the health information privacy protections they can expect at home. Most patients in Asia, Middle East and Africa will be subject to inferior safeguards in privacy protection. Across the globe, health information has a valuable 'second use' market that, if inappropriately disclosed, can result in financial loss as well as physical and social harm to the individuals concerned.

Digital health includes sensors, personal devices with health applications, Internet connections, social networking interfaces, mobile technology, cloud storage and other networks. Personal health data is increasingly being stored and accessed in areas not regulated by health care or privacy laws, excepting a blind trust by all service providers that are ultimately responsible to the person in describing how their PHI is being protected [5]. Service providers in digital health are typically using own business ethics instead of the more stringent health care ethics of practitioners. There is urgent need for global ethical rules and privacy principles that will make digital health trustworthy.

This workshop will, thorough the following list of renowned international speakers from across the globe, present the key areas of concern for addressing the global protection of health information. It will be structured to allow debate from the participants and the collation of ideas, concerns and critical analysis of the proposed way forward.

Workshop Speakers

Dr Peter Croll PhD, FACS, CP, CEng. Chair of Working Group 4 'Security in Health Information Systems', Convener of Health Informatics Society of Australia, 'Protection of Health Information', VIC, **Australia**.

Prof Pekka Ruotsalainen, Vice chair of Working Group 4 'Security in Health Information Systems', Adjunct Prof, Research, Prof Eemeritus, Tampere University **Finland**.

Prof Eike-Henner W. Kluge, PhD, CEO, Ethics Consultants Int., University of Victoria, **Canada**.

Prof Bernd Blobel, Chair of EFMI WGs SSE and EHR, former Vice-Chair of IMIA WG SiHIS, Professor, Medical Faculty, University of Regensburg, **Germany**.

Dr. Najeeb Al-Shorbaji, Director, Department of Knowledge, Ethics and Research, World Health Organization (WHO) Headquarters, Geneva, **Switzerland**.

Paulette Lacroix, HBScN, MPH, CMC, CIPP/C, CIPP/US, PC Lacroix Consulting Inc., North Vancouver, BC, **Canada**.

Dr Tony Sahama BSc, MPhil, PhD, M.Ed(HE) [MACM, SMIEEE, MIBS, MSSA, SMACS, MHISA], Senior Lecturer, Information Security, Queensland University of Tech., Brisbane, QLD, **Australia**.

Prof Mauro Giacomini, PhD, Department of Informatics, Bioengineering, Robotics and System Engineering (DIBRIS), University of Genova, **Italy**

Prof Yukio Kurihara, Kochi Medical School, Kochi University, **Japan**.

IMIA's WG 4 'Security in Health Information Systems'

IMIA's working group 4 on 'Security in Health Information Systems' has been seeking to address global inadequacies for many years. Proposals on minimum standards, guidelines, legislative frameworks, voluntary codes, etc. have been widely debated and published [6].

Health information protection has previously relied on regulated models that are somewhat static. Patients seeking 'confidentiality' place trust in the health professionals who they regard as in control. Yet, today's connected world is not adequately controlled. With digital data, significant measures are required to implement 'Privacy' protection.

More importantly, privacy principles alone are insufficient without monitoring and accountability. This is becoming increasingly evident as data breaches escalate even when organisations appear, on the face of it, to have good protection measures in place. The biggest threat now is the 'human factor' where employees may be naive, ill-informed and careless, disgruntled or simply dishonest.

While professional cyber criminals might be grabbing all the headlines, the dangers presented by internal threats are starting to raise serious concerns among hospitals and clinics. In a 2014 security report by KLAS Research, survey respondents listed unauthorized access and identity management as their number one concern. One provider was quoted as saying, *"Many people think that people on the outside hack into the system, but that is not the case. People who are already on the inside and already have the appropriate access are given $1,000 by outside people to get 100 Social Security numbers"* [7].

Regardless of the country concerned, legislation for health information protection (where it exists) is a patchwork that generally relies on the threat of prosecution to regulate privacy breaches. International standards, and certifications are not integrated into any common framework. International legislation (except the European Union) is virtually non-existent.

Following WG4's previous workshop at MIE2014; it is now the working group's belief that an integrated approach to certification and/or accreditation, specifically for health information protection, is a viable way forward. This workshop will critically discuss these objectives and record the concerns raised by the international participants.

Ways to trustworthy use of PHI in global and networked society

Certification of systems processing PHI, the use of a Trust Authority and Trusted Information Processing Platforms are solutions proposed by researchers and Market research organisations. Certifications made by professionals is not consistent with international standards and, above all, are not enforceable. Certification also exists for web sites, but this too is far from adequate when considering the true demands of health information protection. Mostly current certifications are of a general nature covering a wide range of industry sectors. Only in limited circumstances has it been applied specifically to health information.

Accreditation of healthcare organisations in privacy protection is one possible solution, setting a Gold Standard that aims to help individuals determine which overseas healthcare organisations adequately address health quality and safety issues. A preliminary review undertaken by the authors of all of the JCI accredited organisations of one major medical tourism country showed a complete lack of any Privacy Policy or equivalent. The goal of accreditation in privacy should be to offer standards for securing PHI that have to be met before a healthcare organisation is permitted to offer services internationally. Only accredited organisations would be given a business licence to operate outside their national jurisdictions. This solution requires interfacing with government agencies, and ideally, a UN office established similar to UNICITRAL.

The Way Forward

It is evident that a new trust creation mechanisms is needed that allows meaningful privacy decisions with regard to access, correction, and exclusion based on individual beliefs. The possibility to establish a truly independent body with high credibility backed by rigorous and insightful policies that generates principles and rules for the trusted platform needed for PHI Protection will be discussed. Strengthening IMIA's current collaboration with the World Health Organisation (WHO) is seen as vital in meeting this aim. This workshop will address whether it is appropriate to establish an international not-for-profit company under IMIA and WHO's guidance for certification and/or accreditation of Health Information Protection. Such an initiative could provide IMIA both professional esteem together with a self-sustaining income stream.

As an example, The Medical Tourism Association [8] is a Global non-profit association for the Medical Tourism and International Patient Industry but it *does not provide any privacy policy proposals.* Other organisations such as Certified Medical Tourism Professional (CMTP) and Certified Medical Tourism Specialist (CMTS) give a certification that is valid for (2) years. Unfortunately, those organisations policies waiver patients' moral and privacy rights.

Workshop participants

This workshop will be of general interest to anyone who is responsible for the protection of health information. Those with a technical background in information security will see the relevance of the latest scientific tools and methods for data protection. Participants with an interest in the human factors will rec-

ognise the approaches and values applied to facilitate the effective protection of information privacy. These include the politics, policies and legal frameworks that are of interest to both the general participant and our IMIA leaders.

The IMIA working group members of SiHIS, which typically attract from 30-50 participants, will make up the core attendees.

Contributions from each speaker

The workshop has been structured to follow a previously successful model that will both inform the participants and allow for their interaction. A short introduction will outline the themes and expected outcomes. In the first session, international speakers will give short informative talks on their particular perspective. In the second session, a panel of industry, academia and international government representatives will facilitate viewpoints and respond to questions and answers from the audience. Finally a summary will be presented together with the way forward for ongoing participation.

Dr Peter Croll – Introduction, The key global issues in protecting Health Information – why does it differ, Discussion and Conclusions. Session 2 chair.

Prof Pekka Ruotsalainen – Privacy principles and trust formulation methods for Global protection of PHI, Discussion and Conclusions. Session 1 chair.

Prof Eike-Henner W. Kluge – Health Information Privacy in a Global World: Ethical and legal arguments for the international certification and accreditation of providers and professionals. Panel Member

Prof. Bernd Blobel – Attribute-based and policy-driven access control - how to harmonize across national, jurisdictional and cultural borders, Discussion and Conclusions.

Dr Najeeb Al-Shorbaji, – Development of a model national eHealth law. Panel member.

Paulette Lacroix – Privacy Legislations for Personal Health Information – comparisons and concerns, Discussion and Conclusions. Panel member.

Dr Tony Sahama – Information security and Information Accountability using digital right management protocols. Does this approach work? Socio-Technical Analysis with case studies

Prof Mauro Giacomini – Privacy issues in the use of a Healthcare Services Specification Project (HSSP) platform – an example in an Italian solution for data reuse in Infective Diseases wards.

Prof Yukio Kurihara – Japanese approach to a secure use of personal health information.

Expected results

The workshop identifies barriers, concerns and drafts solutions for the protection PHI at the global level. The discussion especially highlights the importance of the creation of trust mechanisms such as certification, and the need to establish a truly independent body for the development of principles and rules for trusted processing of PHI at global level. Outcomes of the workshop will be published to initiate wider discussion.

At the end of the workshop, the future leaders for SiHIS will be determined and its next year's strategy will be discussed.

Time required

Due to the proposed structure of presentation to include debate and concluding discussions we kindly request the SPC to **assign two time slots for this workshop**. This proposed approach was highly successful at the previous joint EFMI/IMIA workshop at MIE2014 in Istanbul.

References

[1] Corey M. Angst, Ritu Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, MIS Quarterly archive Journal, Volume 33 Issue 2, June 2009 Pages 339-370

[2] Fourth Annual Benchmark Study on Patient Privacy & Data Security, Ponemon Institute LLC, March 2014, see: http://www.ponemon.org/

[3] Business proposal for the Protection of health Information, presented by SiHIS to IMIA General Assembly, Nov 2014.

[4] Rajiv N. Thakkar, Medical Tourism, The Hospitalist, The Society of Hospital Medicine, 2010, see: http://www.the-hospitalist.org/article/medical-tourism/

[5] P Ruotsalainen, B Blobel, Seppälä, P Nykänen1, Trust Information-Based Privacy Architecture for Ubiquitous Health JMIR Mhealth Uhealth 2013;1(2):e23), doi:10.2196/mhealth.2731

[6] K Yamamoto, Y Okuhara, E-H W. Kluge, PR Croll, FR France, P Ruotsalainen, K Ishikawa, The recommendations from the 2009 SiHIS working conference in Hiroshima; Issues on trustworthiness of health information and patient safety, Int Journal of Medical Informatics 8 0 (2011) 75–80

[7] A Holistic Strategy for Preventing Internal Breaches in Patient Data Security, White paper, Caradigm, 2014, see: http://www.caradigm.com/

[8] Medical Tourism Association 2014, see www.medicaltourismassociation.com/en/index.html